10

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,071	12/28/2001	Andrew F. Glew	42390.P13769	5239

7590 04/19/2006

John P. Ward, Esq.
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, CA 90025-1026

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/041,071	**Applicant(s)** GLEW ET AL.	
	Examiner Tamara Teslovich	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

This office action is in response to Applicant's Remarks and Amendments filed January 9, 2006.

Claims 3, 10, 12, and 19 are amended.

Claims 1-34 are herein considered.

Response to Arguments

Applicant's arguments concerning the Examiner's previous Abstract Objections have been fully considered but they are not persuasive.

The abstract of the disclosure remains objected to because it is not an adequate and clear statement of the contents of the disclosure and generally in line with the guidelines. The Applicant's abstract fails to enable the United States Patent and Trademark Office and the public generally to determine quickly from a cursory inspection the nature and gist of the technical

disclosure. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper content of an abstract of the disclosure.

> A patent abstract is **a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains.** If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the

abstract should mention by way of example the preferred modification or alternative.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Applicant's arguments, see page 12 lines 6-30, filed January 9, 2006, with respect to **claims 32-33** have been fully considered and are persuasive. The objection of claim 33 has been withdrawn.

Applicant's amendments to **claims 3 and 10** have been fully considered and are sufficient to overcome the Examiner's previous 35 U.S.C. 112 rejections.

Applicant's arguments, see pages 13-14, filed January 9, 2006, with respect to claims **1-2, 6-9, 12-13, 29-34** have been fully considered but are not persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., executing the authenticated code from the private memory) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Applicant argues that 'the invention of claims 1-2, 6-9, 12-13, and 29-34 may thwart such an attack by transferring the authenticated code module to a private memory and executing the authenticated code module from the private memory' but fails to include within the limitations of the claims wherein the code is executed from the private memory.

Applicant's arguments, see pages 16-17, filed January 9, 2006, with respect to claims **19-21** have been fully considered but are not persuasive. Applicant's arguments are based upon those arguments applied to claim 1 above and are rejected by the Examiner for the same reasons as given above with regards to claim 1.

Applicant's arguments, filed January 9, 2006, with respect to the rejection(s) of claim(s) 3-5, 10-11, 14-18, 22-23, and 24-28 under 35 USC 102(e) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of England et al., Patent No. 6,651,171,B1..

The Examiner's 35 U.S.C. 102(e) rejections of claims 1-2, 6-9, 12-13, 19-21 and 29-34 stand as presented in the previous office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 6-9, 12-13, 19-21 and 29-34 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,401,208 B2 by Davis et al.

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

Regarding **claim 1**, Davis discloses a method comprising transferring an authenticated code module to a private memory and executing the authenticated code module stored in the private memory in response to determining that the authenticated code module stored in the private memory is authentic (col.5 lines 9-16 and 55-67; col.6 lines 1-13).

Regarding **claim 2**, Davis discloses transferring a number of bytes specified by an operand from a memory (col.5 lines 17-65).

Regarding **claim 6**, Davis discloses determining whether the authenticated code is authentic based upon a digital signature of the authenticated code module (col.5 line 66 thru col.6 line 13).

Regarding **claim 7**, Davis discloses obtaining a first value from the authenticated code module stored in the private memory; computing a second value from the authenticated code module; and determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship (col.5 line 65 thru col.6 line 13).

Regarding **claim 8**, Davis discloses retrieving a key decrypting a digital signature of the authenticated code module with the key to obtain a first value, hashing the authenticated code module to obtain a second value; and executing the authenticated code module in response to the first value and the second value having a predetermined relationship (col.5 line 65 thru col.6 line 19).

Regarding **claim 9**, Davis discloses wherein decrypting comprises using the key to RSA-decrypt the digital signature, and hashing comprises apply a SHA-l hash to the authenticated code module to obtain the second value (col.3 lines 37-40; col.4 lines 29-40).

Regarding **claim 12**, Davis discloses retrieving the key from a token (col.4 lines 21-59).

Regarding **claim 13**, Davis discloses receiving the authenticated code module from a machine readable medium (col.4 lines 41-59).

Regarding **claim 19**, Davis discloses A computing device, comprising a chipset, a machine readable medium interface to receive an authenticated code module from a machine readable medium, and a processor coupled to the chipset via a processor bus, the processor to transfer the authenticated code module from the machine readable medium interface to a private memory of the processor and to authenticate the authenticated code module stored in the private memory and to execute the authenticated code module stored in the private memory after authenticating the authenticated code module (col.3 lines 6-55).

Regarding **claim 20**, Davis discloses wherein the private memory is coupled to the processor via a dedicated bus (col.3 lines 14-25; col.4 lines 1-14).

Regarding **claim 21**, Davis discloses wherein the private memory is internal to the processor (col.4 lines 21-59).

Regarding **claim 29**, Davis discloses a machine-readable medium comprising one or more instructions that in response to being executed result in a computing device transferring an authenticated code module to a private memory associated with a processor, and executing the authenticated code module stored in the private memory in response to determining that the authenticated code module stored in the private memory is authentic (col.5 lines 9-16 and 55-67; col.6 lines 1-13).

Regarding **claim 30**, Davis discloses wherein the one or more instructions in response to being executed result in the computing device determining whether the authenticated code is authentic based upon a digital signature of the authenticated code module (col.5 line 66 thru col.6 line13).

Regarding **claim 31**, Davis discloses wherein the one or more instructions in response to being executed result in the computing device obtaining a first value from the authenticated code module stored in the private, computing a second value from the authenticated code module, and determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship (col.5 line 65 thru col.6 line 13).

Regarding **claim 32**, Davis discloses wherein the one or more instructions in response to being executed result in the computing device retrieving an asymmetric key, decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value, hashing the authenticated code module to obtain a second value, and initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship (col.5 line 65 thru col.6 line 19).

Regarding **claim 33**, Davis discloses wherein the one or more instructions comprises a launch instruction that in response to being executed results in the computing device retrieving an asymmetric key, decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value, hashing the authenticated code module to obtain a second value, and initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship (col.5 line 65 thru col.6 line 19).

Regarding **claim 34**, Davis discloses wherein the one or more instructions in response to being executed result in the computing device receiving the authenticated code module via a machine-readable medium interface (col.3 lines 37-40; col.4 lines 29-40).

Claims 1-34 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,651,171 B1 by England et al.

Regarding **claim 1**, England discloses a method comprising transferring an authenticated code module to a private memory and executing the authenticated code module stored in the private memory in response to determining that the authenticated code module stored in the private memory is authentic (col.3 lines 35-43; col3 line 65 thru col.4 line 13; col.7 lines 1-4).

Regarding **claim 2**, England discloses transferring a number of bytes specified by an operand from a memory (col.7 lines 35-56).

Regarding **claim 3**, England discloses configuring a cache memory of a processor to operate as a random access memory, wherein transferring comprises storing the authenticated code module in the cache memory (col.8 lines 15-33).

Regarding **claim 4**, England discloses invalidating the cache memory prior to storing the authenticated code module in the cache memory (col.6 lines 6-67).

Regarding **claim 5**, England discloses locking the cache memory to prevent lines of authenticated code module from being replaced (col.11 lines 40-63).

Regarding **claim 6**, England discloses determining whether the authenticated code is authentic based upon a digital signature of the authenticated code module (col.13 lines 27-40).

Regarding **claim 7**, England discloses obtaining a first value from the authenticated code module stored in the private memory; computing a second value from the authenticated code module; and determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship (col.7 lines 1-34, 57-67).

Regarding **claim 8**, England discloses retrieving a key decrypting a digital signature of the authenticated code module with the key to obtain a first value, hashing the authenticated code module to obtain a second value; and executing the authenticated code module in response to the first value and the second value having a predetermined relationship (col.13 lines 27-40).

Regarding **claim 9**, England discloses wherein decrypting comprises using the key to RSA-decrypt the digital signature, and hashing comprises apply a SHA-I hash to the authenticated code module to obtain the second value (col.13 line 8 thru col.15 line 50).

Regarding **claim 10**, England discloses retrieving the key from a processor used to execute the authenticated code module (col.15 lines 19-52; ol.11 lines 27-39).

Regarding **claim 11**, England discloses retrieving the key from a chipset (col.15 lines 19-52; col.11 lines 27-39).

Regarding **claim 12**, England discloses retrieving the key from a token (col.7 lines 57-67).

Regarding **claim 13**, England discloses receiving the authenticated code module from a machine readable medium (col.6 lines 35-46).

Regarding **claim 14**, England discloses a computing device, comprising a chipset, a memory coupled to the chipset, a machine readable medium interface to receive an authenticated code module from a machine readable medium, a private memory coupled to the chipset, and a processor to transfer the authenticated code module from the machine readable medium interface to the private memory and to authenticate the authenticated code module stored in the private memory (col.3 lines 35-43; col3 line 65 thru col.4 line 13; col.7 lines 1-4).

Regarding **claim 15**, England discloses a memory controller coupled to the memory and a separate private memory controller coupled to the private memory (col.6 lines 5-67).

Regarding **claim 16**, England discloses wherein the chipset comprises a key, and the processor authenticates the authenticated code module stored in the private memory based upon the key of the chipset (col.7 lines 1-34, 57-67; col.15 lines 19-52; col.11 lines 27-39).

Regarding **claim 17**, England discloses wherein the processor comprises a key and authenticates the authenticated code module stored in the private memory based upon the key of the processor (col.15 lines 19-52; col.11 lines 27-39).

Regarding **claim 18**, England discloses a token coupled to the chipset, the token comprising a key, wherein the processor authenticates the authenticated code module stored in the private memory based upon the key of the token (col.7 lines 57-67; col.4 lines 21-59).

Regarding **claim 19**, England discloses a computing device, comprising a chipset (col.7 lines 1-34, 57-67; col.15 lines 19-52; col.11 lines 27-39), a machine readable medium interface to receive an authenticated code module from a machine readable medium (col.6 lines 5-34, 47-67), and a processor coupled to the chipset via a processor bus (col.4 line 51 thru col.5 line 9), the processor to transfer the authenticated code module from the machine readable medium interface to a private memory of the processor, to authenticate the authenticated code module stored in the private memory, and to execute the authenticated code module stored in the private memory after authenticating the authenticated code module (col.3 lines 35-43; col3 line 65 thru col.4 line 13; col.7 lines 1-4).

Regarding **claim 20**, England discloses wherein the private memory is coupled to the processor via a dedicated bus (col.8 lines 16-33).

Regarding **claim 21**, England discloses wherein the private memory is internal to the processor (col.8 lines 16-33).

Regarding **claim 22**, England discloses wherein the private memory comprises internal cache memory of the processor (col.8 lines 15-33).

Regarding **claim 23**, England discloses other processors coupled to the chipset via the processor bus, wherein the processor further locks the processor bus to prevent the other processors from altering the authenticated code module (col.11 line 40 thru col.12 line 10).

Regarding **claim 24**, England discloses a computing device, comprising a memory (col.6 lines 5-34, 47-67), a chipset (col.7 lines 1-34, 57-67; col.15 lines 19-52; col.11 lines 27-39) comprising a memory control that defines a portion of the memory as private memory (col.6 lines 5-34, 47-67), a machine readable medium to receive an authenticated code module from a machine readable medium (col.6 lines 5-34, 47-67), and a processor to transfer the authenticated code module from the machine readable medium interface to the private memory (col.4 line 51 thru col.5 line 9) and to authenticate the authenticated code module stored in the private memory (col.3 lines 35-43; col3 line 65 thru col.4 line 13; col.7 lines 1-4).

Regarding **claim 25**, England discloses wherein the chipset comprises a memory controller coupled to the memory and a separate private memory controller coupled to the private memory (col.6 lines 47-67; col.9 lines 60-67).

Regarding **claim 26**, England discloses wherein the chipset comprises a key, and the processor authenticates the authenticated code module stored in the private memory based upon the key of the chipset (col.15 lines 19-52; col.11 lines 27-39).

Regarding **claim 27**, England discloses wherein the processor comprises a key and authenticates the authenticated code module stored in the private memory based upon the key of the processor (col.15 lines 19-52; col.11 lines 27-39).

Regarding **claim 28**, England discloses a token comprising a key, wherein the processor authenticates the authenticated code module stored in the private memory based upon the key of the token (col.7 lines 57-67; col.4 lines 21-59).

Regarding **claim 29**, England discloses a machine-readable medium comprising one or more instructions that in response to being executed result in a computing device (col.4 lines 45-67) transferring an authenticated code module to a private memory associated with a processor, and executing the authenticated code module stored in the private memory in response to determining that the authenticated code module stored in the private memory is authentic (col.3 lines 35-43; col3 line 65 thru col.4 line 13; col.7 lines 1-4).

Regarding **claim 30**, England discloses wherein the one or more instructions in response to being executed result in the computing device determining whether the authenticated code is authentic based upon a digital signature of the authenticated code module (col.5 line 65 thru col.6 line 19).

Regarding **claim 31**, England discloses wherein the one or more instructions in response to being executed result in the computing device obtaining a first value from the authenticated code module stored in the private, computing a second value from the authenticated code module, and determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship (col.13 line 8 thru col.15 line 50; col.15 lines 45-67).

Regarding **claim 32**, England discloses wherein the one or more instructions in response to being executed result in the computing device retrieving an asymmetric key, decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value, hashing the authenticated code module to obtain a second value, and initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship (col.13 line 8 thru col.15 line 50; col.3 lines 45-52; col.3 lines 45-52; col.15 lines 45-67).

Regarding **claim 33**, England discloses wherein the one or more instructions comprises a launch instruction that in response to being executed results in the computing device retrieving an asymmetric key, decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value, hashing the authenticated code module to obtain a second value, and initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship (col.13 line 8 thru col.15 line 50; col.3 lines 45-52; col.15 lines 45-67).

Regarding **claim 34**, England discloses wherein the one or more instructions in response to being executed result in the computing device receiving the authenticated code module via a machine-readable medium interface (col.6 lines 5-34, 47-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TT

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER